Ellie's cheatsheet & resource dump

Formatted Edition

Original edition here

Table of Contents

General Resources 1

Active Directory & Red Teaming 2

Reverse Engineering. 2

Web Pentesting. 2-3

Miscellaneous. 3-4

Tools and Repositories. 4

More Resources. 4

References. 4-5

General Resources

- The Book of Secret Knowledge
- VX Underground
- Security List
- HackerOne
- HackTricks
- MITRE ATT&CK
- Ired Team
- Sec-Consult
- PayloadsAllTheThings
- Awesome Pentest
- OWASP Cheat Sheets
- Enumeration Guide
- Exploit Notes
- Kernel Exploits
- The Concise Blue Team Cheat Sheets
- Bug Bounty Hunting
- The Hacker Recipes
- Pentester Academy

- Infosec Institute Resources
- Infosec Writeups
- SecurityTube
- Crypto Cat CTF
- Red Team Toolkit
- CTF 101

Active Directory & Red Teaming

- AD Attack Defense
- Active Directory Exploitation Cheat Sheet
- Red Team Handbook
- Red Team Infrastructure Wiki
- Red Team Cheat Sheet
- Red Team Recipe
- Red Team Guides
- Attacking & Securing Active Directory
- Windows & Active Directory Exploitation Cheat Sheet
- Sudoninja Book
- HTB Academy CPTS
- Internal All The Things
- AD Attack & Defense

Reverse Engineering

- Applied Reverse Engineering Series
- Reversing

Web Pentesting

- Total OSCP Guide
- Web Pentesting Enumeration
- Master Web Penetration Testing
- Pentest Lab

Miscellaneous

- Dark Vortex Blog
- Lolbas Project
- Cobalt Blog
- Outflank Publications
- Hacking Life
- Apriorit Dev Blog
- Crypt0ace
- Info-Sec Docs
- Infinitelogins
- Hideandsec
- Zero Infection
- Red Fox Security
- Repos ZENK
- Burmat
- Pwn College
- Security Reference Guide
- The Pentesting Guide
- Infosec Reference
- Guy in a Tuxedo

- AD Exploitation Cheat Sheet
- Attacking AD
- WADCOMS
- Windows Security
- Active Directory Exploitation
- Active Directory Exploitation, 2

Tools and Repositories

- p0wnedLoader
- CSharp, DotNetToJScript, XSL
- PowerShellScripts
- Introduction to PSAmsi
- WmiSploit

More Resources

- COM XSL Transformation: Bypassing Microsoft Application Control Solutions (CVE-2018-8492)
- Disabling AMSI in JScript with One Simple Trick
- oddvar.moe
- Building a Windows Defender Application Control Lab
- Threat Detection using Windows Defender Application Control (Device Guard) in Audit Mode
- Exploring PowerShell AMSI and Logging Evasion
- Device Guard and Application Whitelisting on Windows - An Airing of Grievances
- AMSI Bypass

References

- SNEAKING PAST DEVICE GUARD - Cybereason - Philip Tsukerman
- PowerShell about_Logging_Windows - Microsoft Documentation
- Do You Really Know About LSA Protection (RunAsPPL)? - itm4n - Apr 7, 2021

- Determine the Enterprise Context of an app running in Windows Information Protection (WIP) - 03/10/2023 - Microsoft
- Create and verify an Encrypting File System (EFS) Data Recovery Agent (DRA) certificate - 12/09/2022 - Microsoft
- DISABLING AV WITH PROCESS SUSPENSION - March 24, 2023 - By Christopher Paschen
- Disabling Event Tracing For Windows - UNPROTECT PROJECT - Tuesday 19 April 2022
- ETW: Event Tracing for Windows 101 - ired.team
- Remove Windows Defender Application Control (WDAC) policies - Microsoft - 12/09/2022